DOD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83

DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

COMMANO, CONTROL.
COMMUNICATIONS
AND
INTELLIGENCE

December 26, 1985

FOREWORD

This publication, DoD 5200 .28-STD, “Department of Defense Trusted Computer System Evaluation Criteria,” is issued under the authority .of and in accordance with DoD Directive 5200.28, “Security Requirements for Automatic Data Processing (ADP) Systems,” and in furtherance of responsibilities assigned by DoD Directive 5215.1, “Computer Security Evaluation Center.” Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28.

The provisions of this document apply to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, the Defense Agencies, and activities administratively supported by OSD (hereafter called “DoD Components”).

This publication is effective immediately and is mandatory for use by all DoD Components in carrying out ADP system technical security evaluation activities applicable to the processing and storage of classified and other sensitive DoD information and applications as set forth herein.

Recommendations for revisions to this publication are encouraged and will be reviewed biannually by the National Computer Security Center through a formal review process. Address all proposals for revision through appropriate channels to: National Computer Security Center, Attention: Chief, Computer Security Standards.

DoD Components may obtain copies of this publication through their own publications channels. Other federal agencies and the public may obtain copies from: Office of Standards and Products, National Computer Security Center, Fort Meade, MD 20755-6000, Attention: Chief, Computer Security Standards.

Donald C. Latham

Donald C. Latham
Assistant Secretarv of Defense
(Command, Control, Communications, and Intelligence)

ACKNOWLEDGMENTS

Special recognition is extended to Sheila L. Brand, National Computer Security Center (NCSC), who integrated theory, policy, and practice into, and directed the production of this document.

Acknowledgment is also given for the contributions of: Grace Hammonds and Peter S. Tasker, the MITRE Corp., Daniel J. Edwards, NCSC, Roger R. Schell, former Deputy Director of NCSC, Marvin Schaefer, NCSC, and Theodore M. P. Lee, Sperry Corp., who as original architects formulated and articulated the technical issues and solutions presented in this document; Jeff Makey, formerly NC SC, Warren F. Shadle, NC SC, and Carole S. Jordan, NCSC, who assisted in the preparation of this document; James P. Anderson, James P. Anderson Co., Steven B. Lipner, Digital Equipment Corp., Clark Weissman, System Development Corp., LTC Lawrence A. Noble, formerly U.S. Air Force, Stephen T. Walker, formerly DoD, Eugene V. Epperly, DoD, and James E. Studer, formerly Dept. of the Army, who gave generously of their time and expertise in the review and critique of this document; and finally, thanks are given to the computer industry and others interested in trusted computing for their enthusiastic advice and assistance throughout this effort.

CONTENTS

PART 1: THE CRITERIA

PART II: RATIONALE AND GUIDELINES

PREFACE

The trusted computer system evaluation criteria defined in this document classify systems into four broad hierarchical divisions of enhanced security protection. The criteria provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products. The criteria were developed with three objectives in mind: (a) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications and as a standard for DoD evaluation thereof; (b) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; and (c) to provide a basis for specifying security requirements in acquisition specifications. Two types of requirements are delineated for secure processing: (a) specific security feature requirements and (b) assurance requirements. Some of the latter requirements enable evaluation personnel to determine if the required features are present and functioning as intended. The scope of these criteria is to be applied to the set of components comprising a trusted system, and is not necessarily to be applied to each system component individually. Hence, some components of a system may be completely untrusted, while others may be individually evaluated to a lower or higher evaluation class than the trusted product considered as a whole system. In trusted products at the high end of the range, the strength of the reference monitor is such that most of the system components can be completely untrusted. Though the criteria are intended to be application-independent, the specific security feature requirements may have to be interpreted when applying the criteria to specific systems with their own functional requirements, applications or special environments (e.g., communications processors, process control computers, and embedded systems in general). The underlying assurance requirements can be applied across the entire spectrum of ADP system or application processing environments without special interpretation.

INTRODUCTION

Historical Perspective

In October 1967, a task force was assembled under the auspices of the Defense Science Board to address computer security safeguards that would protect classified information in remote-access, resource-sharing computer systems. The Task Force report, "Security Controls for Computer Systems," published in February 1970, made a number of policy and technical recommendations on actions to be taken to reduce the threat of compromise of classified information processed on remote-access computer systems .[38] Department of Defense Directive 5200.28 and its accompanying manual DoD 5200.28-M, published in 1972 and 1973 respectivley, responded to one of these recommendations by establishing uniform DoD policy, security requirements, administrative controls, and technical measures to protect classified information processed by DoD computer systems.[11; 12] Research and development work undertaken by the Air Force, Advanced Research Projects Agency, and other defense agencies in the early and mid 70's developed and demonstrated solution approaches for the technical problems associated with controlling the flow of information in resource and information sharing computer systems. [1] The DoD Computer Security Initiative was started in 1977 under the auspices of the Under Secretary of Defense for Research and Engineering to focus DoD efforts addressing computer security issues.[37]

Concurrent with DoD efforts to address computer security issues, work was begun under the leadership of the National Bureau of Standards (NBS) to define problems and solutions for building, evaluating, and auditing secure computer systems.[21] As part of this work NBS held two invitational workshops on the subject of audit and evaluation of computer security .[24; 32] The first was held in March 1977, and the second in November of 1978. One of the products of the second workshop was a definitive paper on the problems related to providing criteria for the evaluation of technical computer security effectiveness .[24] As an outgrowth of recommendations from this report, and in support of the DoD Computer Security Initiative, the MITRE Corporation began work on a set of computer security evaluation criteria that could be used to assess the degree of trust one could place in a computer system to protect classified data .[28;29; 35] The preliminary concepts for computer security evaluation were defined and expanded upon at invitational workshops and symposia whose participants represented computer security expertise drawn from industry and academia in addition to the government. Their work has since been subjected to much peer review and constructive technical criticism from the DoD, industrial research and development organizations, universities, and computer manufacturers.

The National Computer Security Center, formerly named the DoD Computer Security Evaluation Center, was formed in January 1981 to staff and expand on the work started by the DoD Computer Security Initiative. [19] A major goal of the National Computer Security Center as given in its DoD Charter is to encourage the widespread availability of trusted computer systems for use by those who process classified or other sensitive information.[1 3] The criteria presented in this document have evolved from the earlier NBS and MITRE evaluation material.

Scope

The trusted computer system evaluation criteria defined in this document apply primarily to trusted, commercially available automatic data processing (ADP) systems. They are also applicable, as amplified below, to the evaluation of existings ystems and to the specification of security requirements for ADP systems acquisition. Included are two distinct sets of requirements: 1) specific security feature requirements; and 2) assurance requirements. The specific feature requirements encompass the capabilities typically found in information processing systems employing general-purpose operating systems that are distinct from the applications programs being supported. However, specific security feature requirements may also apply to specific systems with their own functional requirements, applications or special environments (e. g., communications processors, process control computers, and embedded systems in general). The assurance requirements, on the other hand, apply to systems that cover the full range of computing environments from dedicated controllers to full range multilevel secure resource sharing systems.

Purpose

As outlined in the Preface, the criteria have been developed to serve a number of intended purposes:

- To provide a standard to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements (with particular emphasis on preventing the disclosure of data) for sensitive applications.
- To provide DoD Components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.
- To provide a basis for specifying security requirements in acquisition specifications.

With respect to the second purpose for development of the criteria, i.e., providing DoD components with a security evaluation metric, evaluations can be delineated into two types: (a) an evaluation can be performed on a computer product from a perspective that excludes the application environment; or, (b) it can be done to assess whether appropriate security measures have been taken to permit the system to be used operationally in a specific environment. The former type of evaluation is done by the National Computer Security Center through the Commercial Product Evaluation Process. That process is described in Appendix A.

The latter type of evaluation, i.e., those done for the purpose of assessing a system's security attributes with respect to a specific operational mission, is known as a certification evaluation. It must be understood that the completion of a formal product evaluation does not constitute certification or accreditation for the system to be used in any specific application environment. On the contrary, the evaluation report only provides a trusted computer system's evaluation rating along with supporting data describing the product system's strengths and weaknesses from a computer security point of view. The system security certification and the formal approval/accreditation procedure, done in accordance with the applicable policies of the issuing agencies, must still be followed before a system can be approved for use in processing or handling classified information.[11; 12] . Designated Approving Authorities (DAAs) remain ultimately responsible for specifying 'security of . systems they accredit.

The trusted computer system evaluation criteria will be used directly and indirectly in the certification process. Along with applicable policy, it will be used directly as technical guidance for evaluation of the total system and for specifying system security and certification requirements for new acquisitions. Where a system being evaluated for certification employs a product that has undergone a Commercial Product Evaluation, reports from that process will be used as input to the certification evaluation. Technical data will be furnished to designers, evaluators and the Designated Approving Authorities to support their needs for making decisions.

Fundamental Computer Security Requirements

Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure. " In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. Six fundamental requirements are derived from this basic statement of objective: four deal with what needs to be provided to control access to information; and two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system.

Policy

Requirement 1- SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information.[10] These rules include requirements such as: No person lacking proper personnel security clearance shall obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e. g., based on a need-to-know).

Requirement 2- MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity y level (e. g., classification), and/or the modes of access accorded those subjects who may potentially access the object.

Accountability

Requirement 3- IDENTIFICATION - Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and 'what classes of information' they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system.

Requirement 4- ACCOUNTABILITY - Audit information must be selectively kept and protected so **that actions affecting security can be traced to the responsible party.** A trusted system must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.

Assurance

Requirement 5- ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.

Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life-cycle.

These fundamental requirements form the basis for the individual evaluation criteria applicable for each evaluation division and class. The interested reader is referred to Section 5 of this document, "Control Objectives for Trusted Computer Systems, " for a more complete discussion and further amplification of these fundamental requirements as they apply to general-purpose information processing systems and to Section 7 for amplification of the relationship between Policy and these requirements.

Structure of the Document

The remainder of this document is divided into two parts, four appendices, and a glossary. Part I (Sections 1 through 4) presents the detailed criteria derived from the fundamental requirements described above and relevant to the rationale and policy excerpts contained in Part II.

Part II (Sections 5 through 10) provides a discussion of basic objectives, rationale, and national policy behind the development of the criteria, and guidelines for developers pertaining to: mandatory access control rules implementation, the covert charnel problem, and security testing. It is divided into six sections. Section 5 discusses the use of control objectives in general and presents the three basic control objectives of the criteria. Section 6 provides the theoretical basis behind the criteria. Section 7 gives excerpts from pertinent regulations, directives, OMB Circulars, and Executive Orders which provide the basis for many trust requirements for processing nationally sensitive and classified information with computer systems. Section 8 provides guidance to system developers on expectations in dealing with the covert channel problem. Section 9 provides guidelines dealing with mandatory security. Section 10 provides guidelines for security testing. There are four appendices, including a description of the Trusted Computer System Commercial Products Evaluation Process (Appendix A), summaries of the evaluation divisions (Appendix B) and classes (Appendix C), and finally a directory of requirements ordered alphabetically. In addition, there is a glossary.

Structure of the Criteria

The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security. Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information. Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security-relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the *Trusted Computing Base* (TCB). Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process.

Within each class, four major sets of criteria are addressed. The first three represent features necessary to satisfy the broad control objectives of Security Policy, Accountability, and Assurance that are discussed in Part II, Section 5. The fourth set, Documentation, describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class.

A reader using this publication for the first time may find it helpful to first read Part II, before continuing on with Part 1.